Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 57-69
https://doi.org//

Online ISSN:
Print ISSN:
www.kjcs.com.ng

An Integrated Physical Security to Enhanced Smart Campus Conceptual Framework

Usman Mustapha[1], Khalid Haruna[2], Rabi Mustapha[3] and Habeebah Adamu Kakudi[4]
[1,2,3]Department of Computer Science, Kaduna State University, Nigeria
[4]Department of Computer Science, Faculty of Computer Science and Information Technology, Bayero University Kano, Nigeria
mustaphaabba40@gmail.com, khalid.haruna@kasu.edu.ng, rabichubu@kasu.edu.ng. hakakudi.cs@buk.edu.ng

Abstract

***Background**: A smart campus is an educational institution that uses Internet of things (IoT) devices, sensors, data analytics and other various digital technologies to improve various aspects of campus life such as security, learning experiences, communication etc to create a more connected and efficient campus environment. The quest of excellence in higher education has become inseparably intertwined with the implementation of smart campus solutions as universities and colleges work to develop more connected, intelligent, and responsive settings. The way educational institutions work has changed as a result of the integration of cutting-edge technologies and data-driven solutions, fostering creativity, efficiency, and better learning experiences. Studies have proposed the concept of a smart campus framework and investigated the effect of its implementation on the campus However, one of the often-overlooked aspects while talking about security in a smart campus is the implementation of physical security features Hence, this study bridges the gap **Aim**: The aim of this study is to enhance a conceptual framework of Smart Campus by integrating Physical security features using IoT technology. **Method**: The study integrated physical security features into a smart governance module of Smart Campus by considering three (3) additional factors thus: Radio frequency identification (RFID), Smart lock and Surveilance camera that makes a total of seven (7) factors in the framework. **Results**: The integration of physical security features into smart governance module of the Smart Campus resulted in a robust smart campus framework that give an improved security system on campus thereby promoting a safe campus for all.*

Keywords: *Smart Campus, Smart Governance, Physical Security, Internet of Things, Radio Frequency Identification.*

1. Introduction

In an era defined by rapid technological advancements, the concept of a "Smart Campus" has emerged as a transformative paradigm in education (Cavus et al., 2022). Scholars have defined a smart campus as “A data-oriented, networked, intelligent and collaborative teaching, management and scientific research system based on big data, internet-of-things, mobile internet, and other advanced information technologies.” (Cheng et al., 2022).

The way educational institutions work has changed as a result of the integration of cutting-edge technologies and data-driven solutions, fostering creativity, efficiency, and better learning experiences (Haleem, et al., 2022). The quest of excellence in higher education has become inextricably intertwined with the implementation of smart campus solutions as universities and colleges work to develop more connected, intelligent, and responsive settings (Sneesl, et al., 2022). Current definitions of a smart campus frequently view it

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

as a scale model of a smart city (Awuzie et al., 2021).Recent technical advancements in this age have far-reaching development phases in big data, cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) (Yigitcanlar, et al., 2019).

Higher education institutions have incorporated this technology into their campuses to transform the teaching, learning, and research experiences of faculty, staff, and students. These innovations include new attendance and collaboration methods. (Zhou & Tang, 2022)

According to Sneesl et al. (2022), Smart gadgets that are widely drawing vast application in personal and large commercial contexts and can boost efficiency and convenience are the reason behind the attention that smart education and the sustainable development of smart campuses have received. University education is essentially. The significance of several factors such as the type of education, the pace at which knowledge is acquired, technology infrastructures, adaptability of instructional strategies, and teacher-student interactions in higher education cannot be overemphasized (kariapper 2020).

A smart campus initiative ability to seamlessly integrate the digital and physical domains is essential to its success. The integration of newer technologies in IOT key management yields enhanced security features (Attkan & Ranga, 2022). The importance of physical security in the overall framework of a smart campus cannot be overstated, even though cyber security and digital infrastructure have rightfully received significant attention, the protection of both the virtual and tangible assets within an educational institution is not just a matter of safeguarding data and networks, but also ensuring the safety and well-being of students, staff, and the physical infrastructure itself.In this context, this study seeks to delve into the development of an enhanced conceptual framework for smart campuses with a particular emphasis on the often-overlooked domain of physical security. It attempts to tackle the integration of physical security, acknowledging that cyber and physical security are inseparably linked and necessary for the overall well-being of a smart campus environment.

2. Related Works

2.1. Technology Acceptance Theory

As put forward by Davis (1989, 1993), Technology acceptance theory implies that if an application is expected to be easy to use, the more likely it is that it will be considered useful for the user and the more likely it is that it will stimulate the acceptance of the technology.

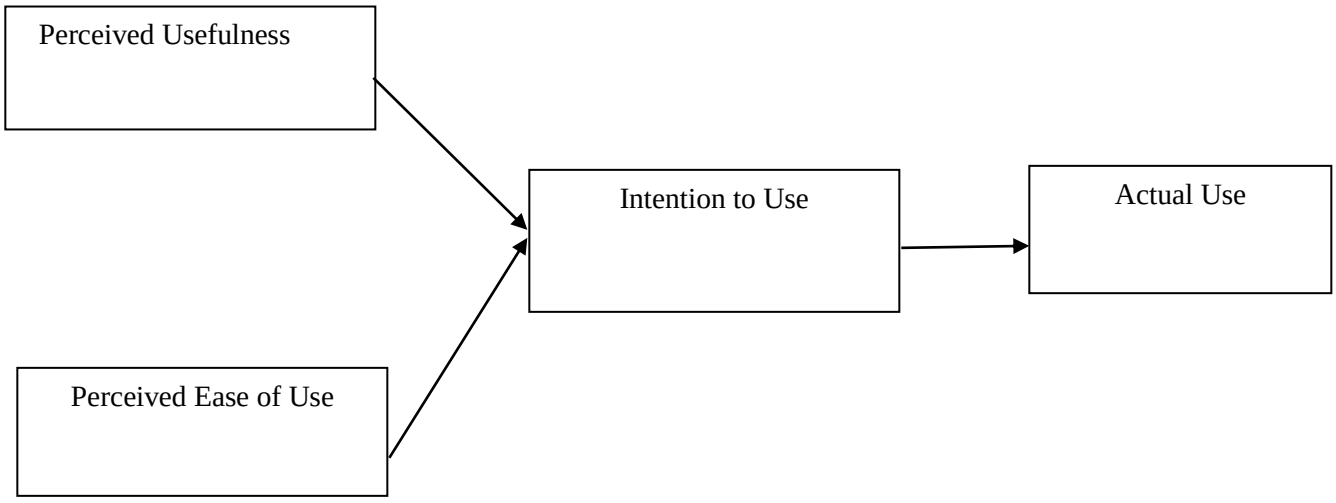

Figure 2.1**.** Technology Acceptance Model (**Source:** Adopted from Marikyan and Papagiannidis (2023).

© The Author(s), under exclusive license to KJCS 2024

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 57-69
https://doi.org//
Online ISSN:
Print ISSN:
www.kjcs.com.ng

The technology acceptance theories and models are designed to predict the individuals' behaviors and measure the degree of acceptance and satisfaction for these individuals against any technology or information system (Momami & Jamous, 2017).

2.2 Conceptual Framework of Smart Campus

The study by Polin et al. (2023), offers a framework made up of four domains that are backed by a broad viewpoint on digital technology and big data. This framework might be viewed as the fifth category in smart campuses that interacts highly with the other four as shown in figure 2.2.

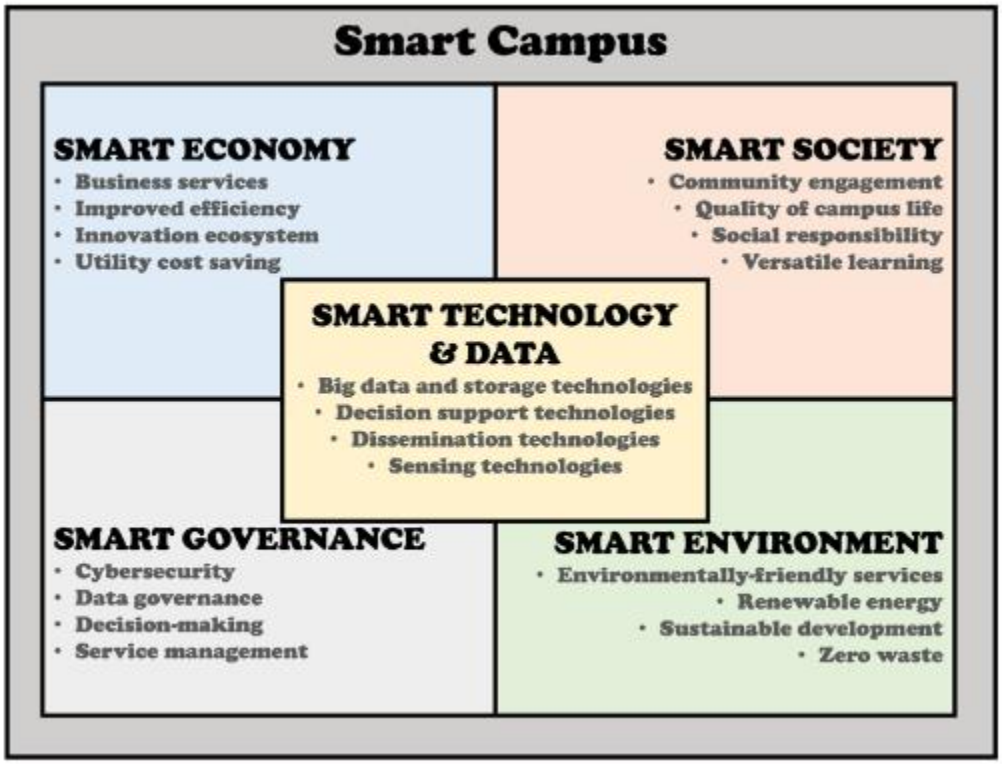

Figure 2.2. Conceptual Framework of Smart Campus (**Source:** Adopted from Polin et al. (2023).

2.2.1 Smart Governance

Potin et al (2023), outlined the governance domain as the means by which the smart campus can be achieved since it entails strategic decision-making and implementation with stakeholder participation. The study notes how the appearance of the "third mission" in higher education led to the role of collaborative governance, which moved from political science and public administration in public policymaking to reaching out to all segments of society by adopting particular public policies through an inclusive approach, users can participate in decision-making and the utilization of public services through the smart campus's governance domain (Fraga-Lamas, 2019). The factors of the governance module were further expatiated into cyber security, data governance, decision-making, and service management which facilitate the governance module.

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

2.2.2 Factors of the Smart Governance

Cyber security

With the rapid rise of IoT, cyber security has become a critical issue for all academic institutions and commercial enterprises. Alzahrani & Bamhdi (2022).

The risks associated with wireless technology and communications from various cyber-attacks have been made clear by numerous researchers and professionals in recent years. These threats can affect both government and private organizations (Kaur & Rankumar, 2022).

A large amount of information is involved in the creation of smart campuses, which highlights the importance of strong cyber security Chen et al. (2022). For smart systems to identify threats in Internet of Things networks, machine learning (ML) and deep learning (DL) intelligence are needed (Alzahrani & Alsaade 2022). However, because they only learn superficially and are unable to defend against fresh attacks, intrusion detection systems (IDS) in online systems that use conventional machine learning methods are growing weaker. Santhi & Kanna (2022), the vast amount of data being generated nowadays is too much for shallow clever algorithms to handle. Because of this, deep learning algorithms are becoming more and more important in current research to handle the growing issue of cloud computing cyber security (Jauro et al., 2020). Deep learning algorithm technologies are being developed quickly in cyber security to address the growing tendency of hacking, additionally, block chain frameworks offer strong defenses against cyberattacks in quantum tools for massive quantum computers with cryptographic components (Polin et al., 2023).

Data Governance

The exercise of authority and control over data management is referred to as data governance (Abraham, Schneider & Brocke 2019). The concept of data governance highlights the important role that data plays in supporting the governing domain in smart campuses, which includes the scientific information system framework that is necessary for these types of campuses (Cao et al., 2022). Data governance facilitates enhance management of information through smart technology.

According to Potin et al. (2023), to develop an intelligent computing model and Internet of Things technology integration system for data detection universities have operational aspects that cater to a diverse range of stakeholders in addition to their conventional roles in teaching and research.

. Information technology is a key component of governance in public enterprises (Telino, et al., 2020). As a result, data governance platforms are necessary for smart campuses in order to manage and control educational data resources in an objective manner (Chen & Liu, 2022). Furthermore, through smart campus innovation and social data governance, there is a need for efficient systems to address the growing issues of student privacy, complicated data, and the digital divide (Cheong & Nyaupane, 2022). Hence, universities are encouraged to fully implement measures to manage large amount of information through big data technology for decision-making and development.

Decision-Making

Pérez et al. (2021), development a smart platform that delivers smart projects using an IT conceptual framework. Which shows how advancement in intelligent technology is beginning to appear in university decision-making.

Through wise decision-making based on objective principles, the robust decision-making produced by smart campuses helps its governance domain (Dong et al., 2016, Polin et al., 2023). To improve the adoption and utilization of IoT-based smart campuses effectively, university administrators, industry, and policymakers need to

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

be aware of the critical issues surrounding smart campuses, which include particular technologies, organizational traits, environmental values, and end user requirements (Sneerl et al., 2022). Furthermore, the goal of a university's usage of smart technology for a smart campus is to prioritize improvement measures and streamline processes that show evolution routes, creating a roadmap that makes decision-making easier (Rico-Bautista et al., 2022). Furthermore, a smart campus can be created to improve administration, management, and decision-making by modeling it after a smart city (Fortes et al., 2019). Therefore, advances in decision-making have embraced the strategy of transforming college campuses into smart cities with a more centralized body for smart governance (Alrashed, 2020) for sustainability management and implementation through an integrated management system to facilitate decision making.

Service Management

In order to facilitate service integrations and build a dynamic digital ecosystem, open extensible architecture was the goal of service management innovation (Adamkó 2018). Artificial intelligence (AI) is therefore utilized to support the university's education function by improving all educational procedures and student accomplishments (Al-Shoqran, & Shorman 2021). An architectural framework for the integration of technologies was developed by Villegas-Ch, et al. (2019) to enhance academic and administrative management. The framework's adaptability allows for the implementation of numerous services in universities. A study by Yee, et al. (2020) on Smart parking development addressed the problem of unauthorized visitors in the campus by enhancing the security service through the coordination of vehicle identification and a novel optimal allocation framework developed to allow a campus manager to re-domain a car park for revenue generation through electric vehicles (Sutjarittham, 2021).

3. Methodology

3.1 The Methodological Stages

The methodological stages are two, thus stage one literature review, stage two, enhancing the framework by integrating physical security as one of the important factor necessary for safety in a smart campus.

3.2.1 Stage I Literature Review

At this stage, the concept of "Smart Cities and Smart Campuses" are understood which identifies the underpinning criteria that define a smart campus in order to adopt the best solution to integrate physical security features using IoT technology that can be adopted by the university community to help identify the most important criteria for the integration of physical security features in a smart campus.

3.2.3 Stage II The enhanced Framework and It Evaluation

In this stage, the framework was enhanced by integrating physical security features using IoT technology
The integration of physical security features into the smart governance framework resulted in a robust smart governance framework which will in turn, bring about an improved security system on campus.

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

4. Result and Discussions

4.1 Enhanced Conceptual Framework

The Figure 4.1 depicted the proposed enhanced Smart Campus Conceptual Framework by Polin et al. (2023).

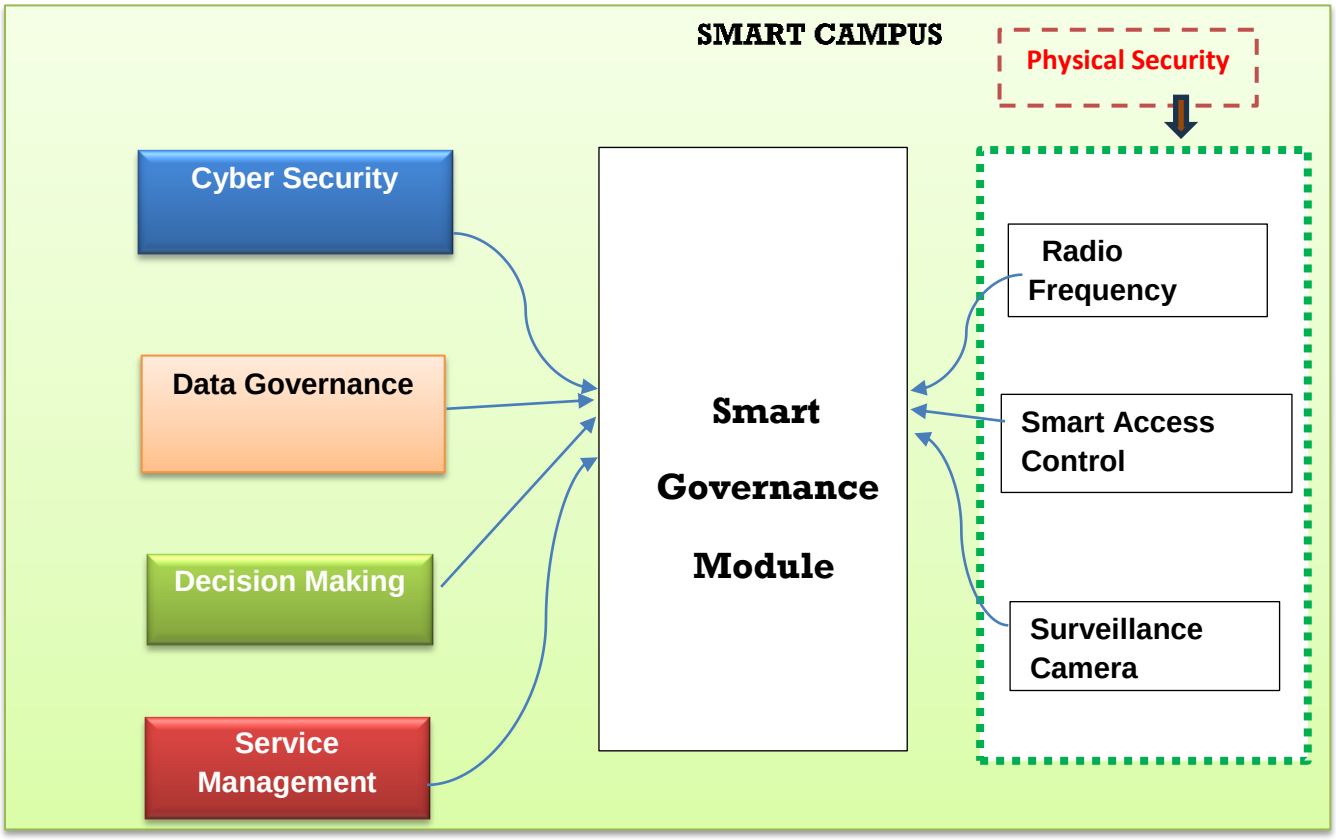

Figure 4.1. Proposed Enhanced Smart Campus Conceptual Framework.

4.2. Factors of The Enhanced Smart Campus Framework

In enhancing the conceptual framework, physical security features was integrated into the smart governance module, using IoT technology such as RFID, Smart Locks and Video Surveillance that served as factors in the module enabled by cloud computing technology used to manage the data from connected device. In exploring the strength of Internet of Things (IoT) functionality in terms of value, veracity, variability, volume of data, and integrating with the

radio-frequency identification (RFID) for human monitoring used for a long-range reading of implanted cards, Video Surveillance for real time monitoring and video analytics in other to trigger alarm in case of unusual activities and Smart door locking will boost the security system deployed to the campus.

© The Author(s), under exclusive license to KJCS 2024

Kasu Journal of Computer Science Vol.1 No.1 [March, 2024], pp. 57-69
https://doi.org//
Online ISSN:
Print ISSN:
www.kjcs.com.ng

Radio Frequency Identification

Both smart cards and Radio Frequency Identification **(**RFID) are extensively used technologies; smartcards provide information processing capabilities and storage capacity, while RFID ensures a simultaneous reading of the recognized objects (Beqqal et al. 2017).

According to Ishaq & Bibi (2022), Radio Frequency Identification (RFID) technology is widely used in a variety of industries and enterprises, such as transportation, smart cities, retail sales, and agricultural. Additionally, educational institutions have started using RFID to track student attendance combining this technology with Google Sheets and the Internet of Things (IoT) to build a real time attendance tracking system. For a comprehensive analysis of the development of an attendance system for students. Unlike the traditional attendance system, which relies on handwritten signatures, this RFID-based system allows automation, removing a number of issues related to the manual procedure, including time wastage, proxies, and the potential for the attendance sheet to be lost. By developing a system that allows students to simply flash their student IDs at the RFID reader to have their attendance immediately registered

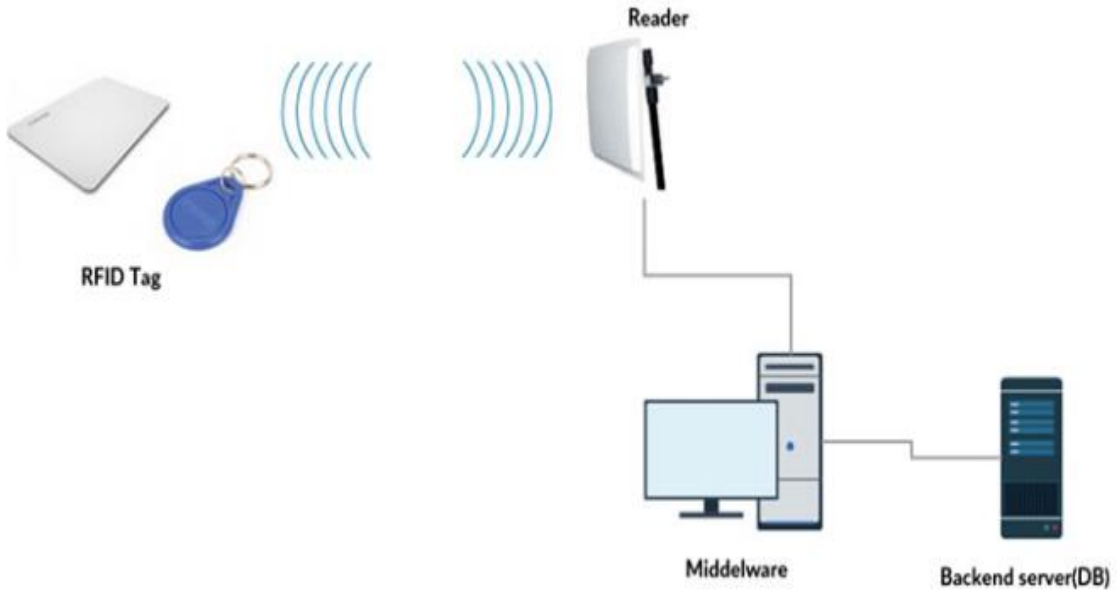

Figure 4.2. General Architecture of RFID based System (**Source**: Beqqal et al. (2017)).

.

According to Beqqal et al. (2017), RFID stands for radio frequency identification, a quick and automatic identification technique that detects tags on items by using radio frequency when the tags are in close proximity to an RFID reader. The general architecture of an RFID-based system is shown in Figure 4.2. As stated, an RFID system comprises:

1. Tag, consist of a chip, antenna and a certain amount of computational and storage capabilities
2. Reader, interrogates tag to obtain tag information and forwards the encrypted information gathered from the tag to the backend server for verification purpose.
3. Software responsible to gather data from reader, and dispatch it to the backend servers.

Backend server contains a local database and some processors. One benefit of utilizing RFID technology is that it can read multiple labels at once and save data, such as a student's ID (Beqqal et al., 2017).

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

Access control systems should be employed in institutions where security is a top priority and access to certain areas needs to be verified. This will improve security overall and cut down on the amount of time it takes to verify the credentials of a large number of applicants at once (Beqqal et al., 2017).

Beqqal et al. (2017), presents an access control solution that blends synchronous and asynchronous data processing with particular identification and authentication technologies. In this instance, we focus on the academic setting. We illustrate with two use scenarios the potential security gains from a complimentary combination of RFID and Smartcards. For this reason, the first scenario of our system's design is on verifying students' attendance in tests through the use of synchronous and asynchronous methods based on the integration of RFID and smart card technologies. The second scenario, which is based on RFID technology and staff fingerprints, focuses on the security of entering sensitive regions by offering a synchronous verification approach that demands instantaneous authentication of the access. Additional technologies, such webcams and liveness sensors, are also employed to provide precise authentication.

Habbu et al. (2020, employed Radio Frequency Identification technology as the infrastructure to address the issue of student attendance delays in most universities, which are resolved by calling the roll. The study observed the difficulties with this approach and suggested a new, alternative IoT-based system to manage staff and student attendance. Considering many aspects like time savings, dependability, efficiency, and ease of management, the college administration can better enhance the university's monitoring framework in the indoor environment.

Smart Access Control

Smart locks and access control systems can be managed remotely through IoT, allowing authorized personnel to grant or revoke access as needed. Notifications are received when a secured area is entered.

Hoque and Davidson (2019), developed an architecture for a smart door sensor that will inform a user through an Android application. Similarly, Algamdi, Thanoon, and Alsulami, (2019), proposed a security framework for university campuses, claiming that the use of sensors and drone cameras could ensure campus and stakeholder security. However, taking into account the difficulties brought about by such technology also presents political, technical, and financial difficulties. Shivaraj et al.(2017), focuses on the challenges management faces in keeping track of and controlling everything that occurs on campuses that are dispersed over a big area. They stressed the need of adopting IoT technology in campus using secured smart system for campus academics. In this system sensors are enabled and network devices work continuously and collaboratively to give humans more comfort. Information is gathered by the smart classroom and saved as digital data in the e-campus platform's memory. Here, a platform for engaging learning is developed using e-campus security.

Surveillance Cameras

According to Anagnostopoulos et al., (2021), one of the most important prerequisites for ensuring an uninterruptible, secure operation of a smart campus is the protection of daily routines and activities in an environment that is closely watched by a strong surveillance system. Remote access to real-time video streams is possible with IoT-enabled cameras. Additionally, they can recognize objects with AI and send out threat alerts (Liu et al. 2021).

According to Shahriar et al. (2019), installing a CCTV camera system is a very common way to maintain building or area surveillance. The difficulty with conventional security systems, they pointed out, is that the cameras merely capture and transmit the video feed, making it impossible for someone to view what was happening there at that same moment. However, it is unable to stop burglaries or notify the authorities right away. In their study, the suggested using live video surveillance to identify any person within an institutional building. The system also offers fire alarm, anti-theft protection, and weather report and weapon detection facility. Their method can identify a face in any background from security camera footage, be it that of a teacher, student, or something else

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

entirely from previously saved data on the server. This solution operates with IP cameras that are already deployed in the building at various lighting levels without causing any noticeable errors. They used the RaspberryPi to implement this project with Python libraries such as numPY and OpenCV. For database management, SQLite is utilized. In addition to sending fire alarms and detecting theft and unauthorized personnel, this system can also identify illicit weapons. The whereabouts of every person will be logged by this system in real time. With the aid of Java, a software system is also created to make it easier for the administrator to access the system. Furthermore, in the event that prompt action is required, the GSM module will notify the security authorities by phone or message.

5. Conclusion

The study investigates how a smart governance module can be enhanced in a smart campus framework. The Physical security features is integrated into an already-existing smart governance module of the framework. This emphasizes the importance of this integration in enhancing security on campus through an examination and review of relevant literatures. IoT technology such as RFID, Smart lok and surveillance camera and its overall efficiency were utilized to provide a robust smart campus framework that give an improved security system on campus.The study advances the implementation of physical security methods in the era of an improved smart campus by offering useful suggestions and addressing some important physical security threats.

Implementing physical security like RFID technology, smart locks and surveillance cameras can significantly improve security in a campus environment by restricting unauthorized access, providing real time monitoring, and deterring potential threats. By so doing, a safer environment for students, staff and visitors is created thereby promoting a safe and conducive environment for community engagement and learning.

However, the future work of this study will embark on the evaluation of the proposed framework by validation method.

Reference

Abraham, R., Schneider, J., & Brocke, J. V. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008.

Adamkó, A. (2017). Building smart university using innovative technology and architecture. In *Smart innovation, systems and technologies*. https://doi.org/10.1007/978-3-319-59454-5_6.

Algamdi, A., Thanoon, M.I., & Alsani, A. (2019). Toward s Smart Campus using IoT: Framework for safety and security system on a university campus. *Advances in Science Technology and Engineering Systems Journal, 4(5). 97-103.* https://doi.org.10.25046/aj04512.

Alrashed, S. (2020). Key performance indicators for Smart Campus and Microgrid. *Sustainable Cities and Society*, *60*, 102264. https://doi.org/10.1016/j.scs.2020.102264.

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

Al-Shoqran, M., & Shorman, S. (2021). A review on smart universities and artificial intelligence. In *Studies in computational intelligence* (pp. 281–294). https://doi.org/10.1007/978-3-030-62796-6_16.

Alzahrani, M., & Bamhdi, A. M. (2022). Hybrid deep-learning model to detect botnet attacks over internet of things environments. *Soft Computing*, *26*(16), 7721–7735. https://doi.org/10.1007/s00500-022-06750-4.

Al-Zahrani, M. S., & Alsaade, F. W. (2022). Computational intelligence approaches in developing cyberattack detection system. *Computational Intelligence and Neuroscience*, *2022*, 1–16. https://doi.org/10.1155/2022/4705325.

Anagnostopoulos, T., Kostakos, P., Zaslavsky, A., Kantzavelou, I., Tsotsolas, N., Salmon, I., Morley, J., & Harle, R. (2021). Challenges and Solutions of Surveillance Systems in IoT-Enabled Smart Campus: A survey. *IEEE Access*, *9*, 131926–131954. https://doi.org/10.1109/access.2021.3114447.

Attkan, A.& Ranga, V.(2022).Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security https://doi.org/10.1007/s40747-022-00667-z

Awuzie, B., Ngowi, A., Omotayo, T., Obi, L., & Akotia, J. (2021). Facilitating successful smart Campus Transitions: A Systems Thinking-SWOT Analysis approach. *Applied Sciences*, *11*(5), 2044. https://doi.org/10.3390/app11052044.

Bautista, D. R., Guerrero, C. D., Collázos, C. A., Maestre-Góngora, G., Sánchez-Velásquez, M. C., Medina-Cárdenas, Y., Sánchez, D. T. P., Barreto, A. G., & Swaminathan, J. (2022). Key Technology Adoption Indicators for Smart Universities: A Preliminary proposal. In *Lecture notes in networks and systems* (pp. 651–663). https://doi.org/10.1007/978-981-16-6309-3_61.

Beqqal, M. E., Kasmi, M. A., & Azizi, M. (2016). Access control system in campus combining RFID and biometric based smart card technologies. In *Advances in intelligent systems and computing*. https://doi.org/10.1007/978-3-319-46568-5_56

Cao, H., He, H., & Tian, J. (2022). A scientific research information system via intelligent blockchain technology for the applications in university management. *Mobile Information Systems*, *2022*, 1–14. https://doi.org/10.1155/2022/7512692

Çavuş, N., Mrwebi, S. E., Ibrahim, I. M., Modupeola, T., & Reeves, A. Y. (2022). Internet of Things and its Applications to Smart Campus: A Systematic Literature review. *International Journal of Interactive Mobile Technologies*, *16*(23), 17–35. https://doi.org/10.3991/ijim.v16i23.36215.

Chen, Z., & Liu, Y. (2021). Research and construction of university data governance platform based on smart campus environment. *2021 3rd International Conference on Artificial Intelligence and Advanced Manufacture*. https://doi.org/10.1145/3495018.3495097

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

Chen, Z., Zhou, M., Feng, L., & Li, B. (2022). Statistical Analysis of threatening IP in Universities Based Automated Script. *Proceedings of the 2022 2nd International Conference on Control and Intelligent Robotics*. https://doi.org/10.1145/3548608.3559315.

Cheng, Y., Wei, J., Tan, X., Tan, Y., & Lei, Y. (2022). Research on key technologies of data-oriented intelligent campus in 5G environment. *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*. https://doi.org/10.1109/iccece54139.2022.9712690.

X., Kong, X., Zhang, F., Chen, Z., & Kang, J. (2016). OnCampus: a mobile platform towards a smart campus. *SpringerPlus*, *5*(1). https://doi.org/10.1186/s40064-016-2608-4.

Fortes, S., Santoyo-Ramón, J. A., Palacios, D., Baena, E., Mora-García, R., Medina, M. Á., Mora, P., & Barco, R. (2019). The campus as a Smart City: University of Málaga Environmental, learning, and Research Approaches. *Sensors*, *19*(6), 1349. https://doi.org/10.3390/s19061349.

Fraga- Lamas, P., Celaya-Echarri, M., López-Iturri, P., Castedo, L., Azpilicueta, L., Aguirre, E., Suárez-Albela, M., Falcone, F., & Fernández- Caramés, T. M. (2019). Design and experimental validation of a LORAWAN FOG Computing based architecture for IoT enabled smart campus applications. *Sensors*, *19*(15), 3287. https://doi.org/10.3390/s19153287.

Habbu, N, G., Santosh Kumar M.T., Shreekala Tatachar K S., & Varshitha, R. (2020). Smart Campus Using RFID. International ***Journal of Computer science engineering Techniques-– Volume 5 Issue 2, 2020.***

Haleem, A., Javaid, M., Qadri, M. A., & Suman, R. (2022). Understanding the role of digital technologies in education: A review. *Sustainable Operations and Computers*, *3*, 275–285. https://doi.org/10.1016/j.susoc.2022.05.004.

Hoque, M.A., & Davidson, C. (2019). Design and Implementation of an IoT-Based smart home security. *International Journal of Networks and Distributed Computing. 7(2).* 85. https://doi.org/10.2991/ijndc.k.190326.004.

Ishaq, K., & Bibi., S. (2022), IoT based smart attendance system using RFID: A Systematic Literature Review

Jauro, F., Chiroma, H., Gital, A. Y., Almutairi, M., Abdulhamid, S. M., & Abawajy, J. (2020). Deep learning architectures in emerging cloud computing architectures: Recent development, challenges and next research trend. *Applied Soft Computing*, *96*, 106582. https://doi.org/10.1016/j.asoc.2020.106582

Kanna, P. R., & Santhi, P. (2022). Hybrid Intrusion Detection using MapReduce based Black Widow Optimized Convolutional Long Short-Term Memory Neural Networks. *Expert Systems With Applications*, *194*, 116545. https://doi.org/10.1016/j.eswa.2022.116545

Karriapper, R.K.A.R. (2020) Smart Universities: A technological Framework.*Journal of critical Reviews ISBN-2394-5125. Vol 7, Issue 13, 2020*

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

Kaur, J., & Ramkumar, K. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5766–5781. https://doi.org/10.1016/j.jksuci.2021.01.018.

Zhou, L., & Tang, Q. (2022). Construction of a Six-Pronge intelligent Physical Education classroom model in colleges and universities. *Scientific Programming*, *2022*, 1–11. https://doi.org/10.1155/2022/9003864.

Liu, Y., Kong, L., Chen, G., Xu, F., & Wang, Z. (2021). Light-weight AI and IoT collaboration for surveillance video pre-processing. *Journal of Systems Architecture*, *114*, 101934. https://doi.org/10.1016/j.sysarc.2020.10193.

Marikyan, D. & Papagiannidis, S. (2023). Technology Acceptance Model: A Review. *In S. Papagianidis (Ed), TheoryHubBook.* https://open.ncl.ac.uk/ISBN:9781739604400

Pérez, F. M., Martínez, J. V. B., & Fonseca, I. L. (2021). Modelling and Implementing Smart Universities: an IT Conceptual Framework. *Sustainability*, *13*(6), 3397. https://doi.org/10.3390/su13063397.

Polin, K., Yiğitcanlar, T., Limb, M., & Washington, T. L. (2023). The Making of Smart Campus: A review and Conceptual framework. *Buildings*, *13*(4), 891. https://doi.org/10.3390/buildings13040891.

Shahriar, T.R., Paul, R., Mustakim, & Hassan, F.B. (2019). Smart Video Surveillance System for University Campus. **Technical Report** · September 2019 DOI:10.13140/RG.2.2.22080.25601

.

Sneesl, R., Jusoh, Y. Y., Jabar, M. A., Abdullah, S., & Bukar, U. A. (2022). Factors affecting the adoption of IoT-Based smart Campus: An investigation using Analytical Hierarchical Process (AHP). *Sustainability*, *14*(14), 8359. https://doi.org/10.3390/su14148359.

Sneesl, R.; Jusoh, Y.Y.; Jabar M.A.; Abdullah, S. Revising Technology Adoption Factors for IoT-Based Smart Campuses: A Systematic Review. Sustainability **2022**, 14,4840. https://doi.org/10.3390/su14084840.

Shivaraj Kumar T.H, Sriraksha T. A, Noor U saba. "An IOT Based Secured Smart e-Campus" International Journal of Humanities and Social Science Invention ISSN, Volume 6 Issue, March. 2017, PP.88-93.

Sutjarittham, T. Modelling and Optimisation of Resource Usage in an IoT Enabled Smart Campus. Ph.D. Thesis, UNSW, Sydney, Australia, 2021.

Telino, V., Massa, R., Mota, I., Gomes, A. S., & Moreira, F. (2020). A methodology for creating a macro action plan to improve IT use and its governance in organizations. *Information*, *11*(9), 427. https://doi.org/10.3390/info11090427.

Villegas-Ch, W., Palacios-Pacheco, X., & Luján-Mora, S. (2019). Application of a Smart City Model to a Traditional University Campus with a Big Data Architecture: A Sustainable Smart Campus. *Sustainability*, *11*(10), 2857. https://doi.org/10.3390/su11102857.

© The Author(s), under exclusive license to KJCS 2024

Online ISSN:
Print ISSN:
www.kjcs.com.ng

Yee, O. C., Yaakob, N., Elshaikh, M., & Azahar, F. (2020). A cloud-based automated parking system for smart campus. *IOP Conference Series*, *767*, 012049. https://doi.org/10.1088/1757-899x/767/1/012049.

Yiğitcanlar, T., Marques, J. S., da- Costa, E. M., Kamruzzaman, M., & Ioppolo, G. (2019). Stimulating technological innovation through incentives: Perceptions of Australian and Brazilian firms. *Technological Forecasting and Social Change*, *146*, 403–412. https://doi.org/10.1016/j.techfore.2017.05.039.

© The Author(s), under exclusive license to KJCS 2024